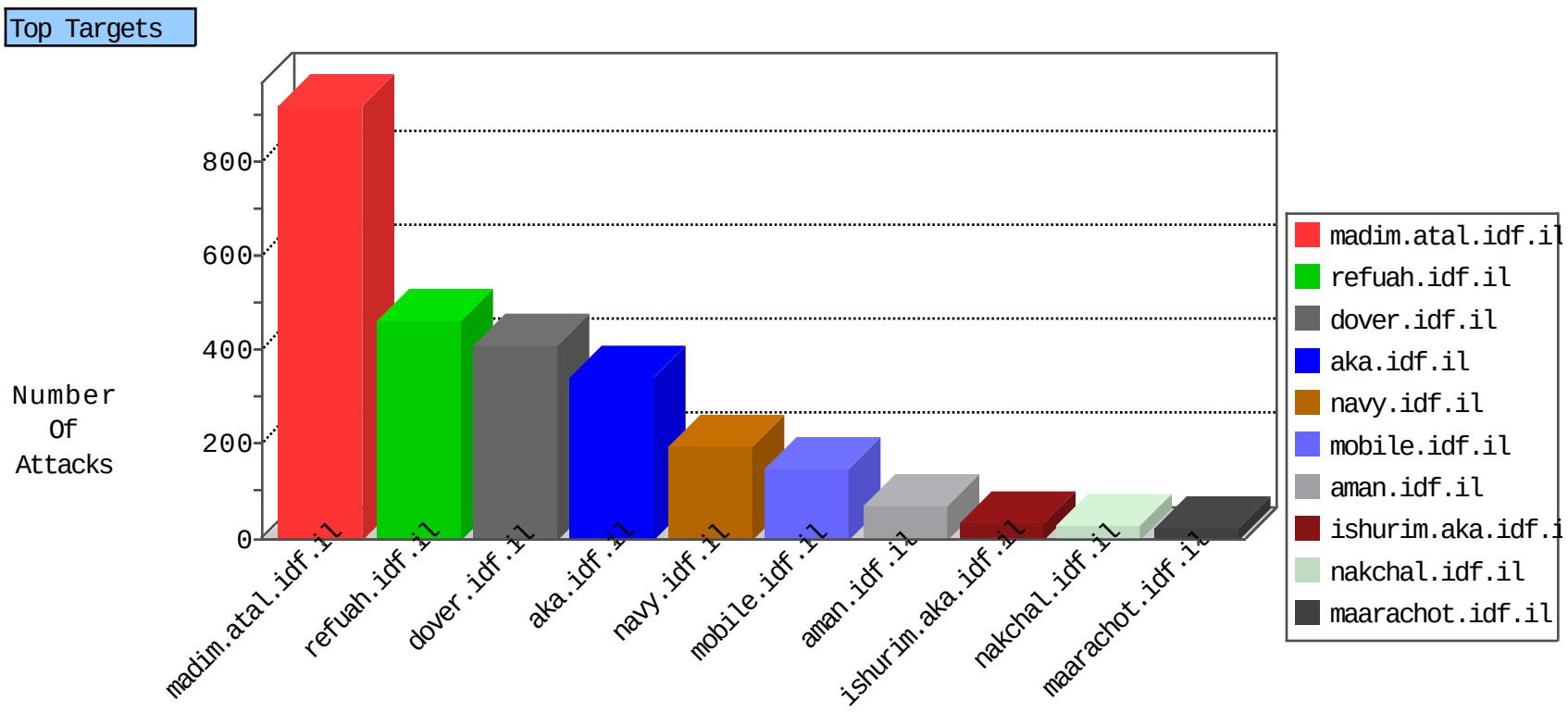
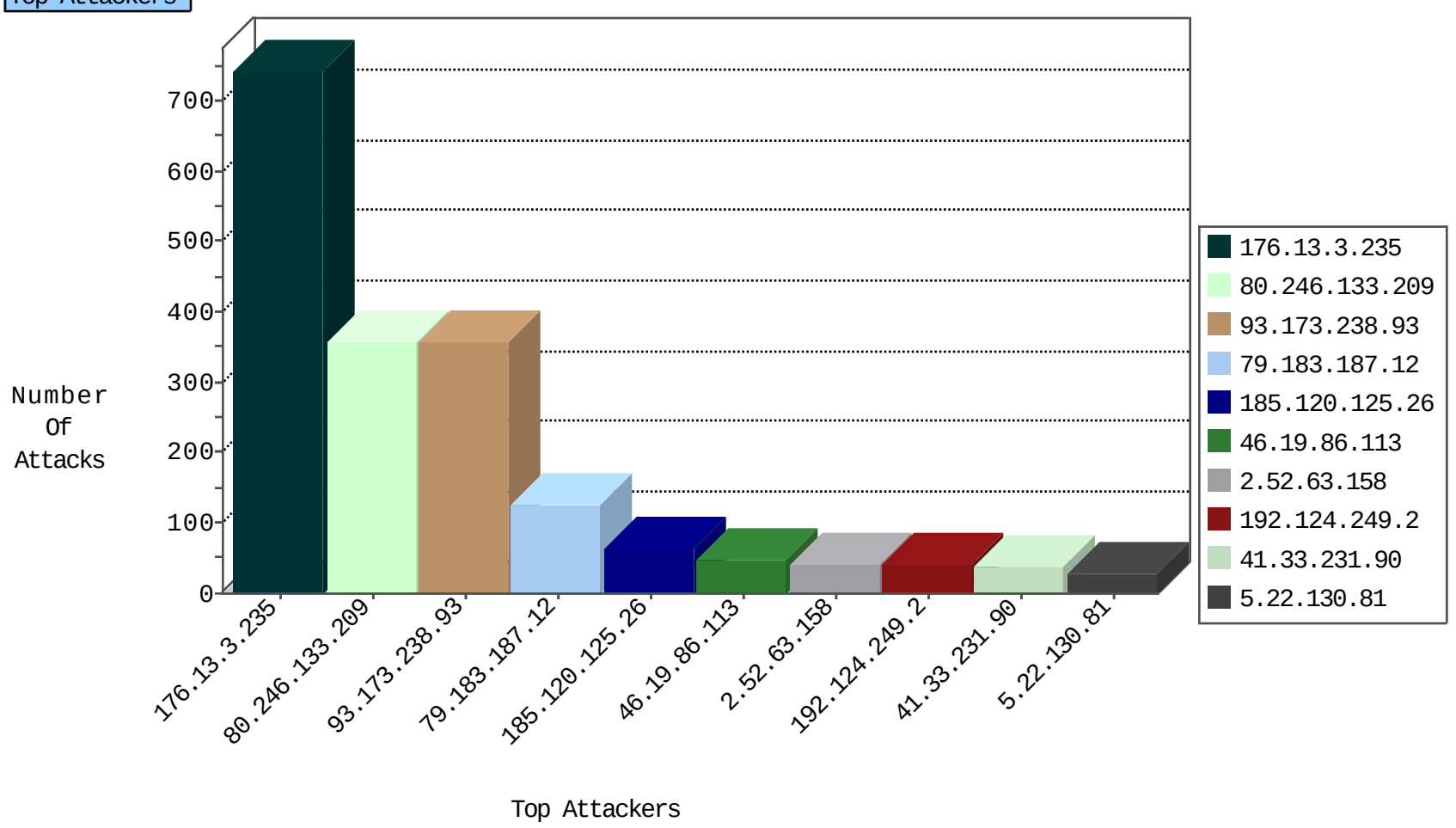
02-07-2016-17:04:07 to 02-07-2016-18:04:07

IDF Under Attack Daily Report

Top Targets



Top Attackers



02-07-2016-17:04:07 to 02-07-2016-18:04:07

Top Attackers In DDoS-Defence

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
81.218.241.26	Israel	147.237.72.166	aka.idf.il	Anomaly-TLS-renegotiation-Cli	dest-reset	118
105.158.109.251	Morocco	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	3
54.72.73.168	Ireland	147.237.77.216	dover.idf.il	SYN Flood out of context	drop	3
109.65.105.6	Israel	147.237.72.156	aman.idf.il	Block_Udp_All_Nets	drop	3
109.65.105.6	Israel	147.237.72.166	aka.idf.il	Block_Udp_All_Nets	drop	3
142.54.160.210	United States	147.237.77.205	prisha.idf.il	block-sp-traf1	drop	1
185.7.227.196	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1
142.54.160.212	United States	147.237.72.167	ishurim.aka.idf.il	block-sp-traf1	drop	1
222.70.208.157	China	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
142.54.169.163	United States	147.237.77.176	matpash.idf.il	block-sp-traf1	drop	1
71.6.135.131	United States	147.237.76.39	mobile.meitav.idf.il	Block_Udp_All_Nets	drop	1
185.7.227.195	United Kingdom	147.237.77.216	dover.idf.il	Invalid TCP Flags	drop	1

02-07-2016-17:04:07 to 02-07-2016-18:04:07

Top Attackers In IPS

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
83.218.232.238	Ukraine	147.237.72.166	aka.idf.il	C106: HTTP: majestic bot	Block	1

02-07-2016-17:04:07 to 02-07-2016-18:04:07

Top Attackers In IDS

Attacker Address	Target Address	Attacker Country	Site	Signature	Count
37.46.35.113	147.237.72.156	Israel	aman.idf.il	ET SCAN NMAP -sA (2)	16
195.34.150.18	147.237.77.216	Austria	dover.idf.il	Tehila - Perl LWP with fake user agent	2
78.193.2.8	147.237.8.50	France	e.tikshuv.idf.il	ET SCAN NMAP -sS window 1024	1
75.159.188.149	147.237.72.217	Canada	e.idf.il	ET SCAN NMAP -sS window 1024	1
217.194.198.104	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
213.8.204.61	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
2.52.136.32	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
209.126.116.147	147.237.77.216	United States	dover.idf.il	ET SCAN NMAP -sS window 1024	1
109.186.185.197	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
94.230.86.245	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
89.138.84.201	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
80.178.159.169	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
77.126.95.208	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1
37.142.228.172	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
213.57.105.47	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
5.29.121.63	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
212.235.98.139	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
109.67.140.14	147.237.77.216	Israel	dover.idf.il	portscan: TCP Distributed Portscan	1
93.189.26.18	147.237.77.170	Austria	maarachot.idf.il	ET SCAN NMAP -sS window 1024	1
80.246.136.25	147.237.72.166	Israel	aka.idf.il	portscan: TCP Distributed Portscan	1

02-07-2016-17:04:07 to 02-07-2016-18:04:07

Top Attackers In FW

Attacker Address	Attacker Country	Target Address	Site	Signature	Message	Device Action	Count
80.246.133.209	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	356
46.19.86.113	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	47
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	44
93.173.238.93	Israel	147.237.76.86	navy.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	38
41.33.231.90	Egypt	147.237.77.216	dover.idf.il	drop	SAM rule	drop	36
2.52.63.158	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	monitor	27
106.218.148.216	India	147.237.77.170	maarachot.idf.il	drop	First packet isn't SYN	drop	24
5.22.130.81	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	Invalid ACK number	monitor	24
185.120.125.26		147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	21
93.173.238.93	Israel	147.237.77.216	dover.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	21
192.124.249.2		147.237.72.156	aman.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
192.124.249.2		147.237.76.147	chinuch.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	20
176.13.1.173	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
80.246.136.15	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	18
149.50.98.136	United States	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	13
2.52.63.158	Israel	147.237.77.243	mobile.idf.il	Bad TCP sequence	Invalid ACK number	alert	13
46.19.86.55	Israel	147.237.76.200	eitan.aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
85.130.253.120	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
66.249.78.216	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	12
37.26.147.157	Israel	147.237.72.167	ishurim.aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	11
212.143.142.56	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
62.219.165.208	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	9
192.116.199.42	Israel	147.237.77.216	dover.idf.il	drop	First packet isn't SYN	drop	9
81.218.241.26	Israel	147.237.72.166	aka.idf.il	drop	First packet isn't SYN	drop	8
79.181.215.57	Israel	147.237.76.31	nakchal.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	8
46.19.86.7	Israel	147.237.72.167	ishurim.aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	8
85.250.234.87	Israel	147.237.77.234	halag.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	8
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	monitor	7
46.19.86.74	Israel	147.237.76.42	refuah.idf.il	drop	First packet isn't SYN	drop	7
46.19.85.122	Israel	147.237.77.216	dover.idf.il	Bad TCP sequence	Invalid ACK number	alert	7
2.54.57.63	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
2.54.3.92	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.19.86.74	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	6
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	SYN retransmit with different window scale	monitor	6
79.178.102.224	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
84.108.74.35	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
46.19.86.74	Israel	147.237.76.42	refuah.idf.il	Bad TCP sequence	SYN+ACK retransmit with different window scale	monitor	6
80.246.137.99	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.176.23.231	Israel	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
46.242.78.131	Russian Federation	147.237.77.74	law.idf.il	drop	First packet isn't SYN	drop	6
80.246.137.140	Israel	147.237.72.166	aka.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	6
157.55.39.251	United States	147.237.77.243	mobile.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
79.180.15.5	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
54.244.22.103	United States	147.237.77.176	matpash.idf.il	drop	First packet isn't SYN	drop	6
2.52.162.196	Israel	147.237.72.166	aka.idf.il	Streaming Engine: TCP Invalid Retransmission	Invalid segment retransmission. Packet dropped.	drop	6
195.34.150.18	Austria	147.237.77.216	dover.idf.il	Block HTTP Non Compliant	Failed to handle connection data	monitor	5
94.230.86.38	Israel	147.237.72.166	aka.idf.il	Bad TCP sequence	Invalid ACK number	monitor	5
46.19.85.243	Israel	147.237.76.42	refuah.idf.il	SYN Attack	SYN -> SYN-ACK -> RST	reject	5
85.65.205.37	Israel	147.237.77.233	atal.idf.il	SYN Attack	SYN -> SYN-ACK -> Timeout	reject	5
212.199.106.194	Israel	147.237.72.167	ishurim.aka.idf.il	drop	First packet isn't SYN	drop	5

02-07-2016-17:04:07 to 02-07-2016-18:04:07

Top Attackers In WAF

Attacker Address	Attacker Country	Target Address	Site	Signature	Device Action	Count
176.13.3.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	419
176.13.3.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	161
176.13.3.235	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (403)	Block	159
93.173.238.93	Israel	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 93.173.238.93	Block	150
93.173.238.93	Israel	147.237.76.86	navy.idf.il	Multiple Unauthorized URL Access from 93.173.238.93	Block	148
79.183.187.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	90
79.183.187.12	Israel	147.237.0.19	madim.atal.idf.i	Distributed Too Many of the Same Response Code (404)	Block	36
109.253.146.247	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	16
2.54.157.18	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	15
79.181.215.57	Israel	147.237.76.31	nakchal.idf.il	Unauthorized HTTP Method	Block	8
79.181.215.57	Israel	147.237.76.31	nakchal.idf.il	Multiple Unauthorized URL Access from 79.181.215.57	Block	7
80.246.136.15	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	6
2.54.135.218	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	6
171.25.193.132	Sweden	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/watch	Block	5
176.13.1.173	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	5
46.19.86.61	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	3
178.32.53.53	United Kingdom	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/watch	Block	3
72.9.148.10	United States	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/994-8613-he/navy.aspx.aspx	Block	2
109.253.222.183	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.178.207.163	Ukraine	147.237.77.216	dover.idf.il	Distributed PHP Attempt	Block	2
176.13.11.135	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.178.207.163	Ukraine	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/xmlrpc.php	Block	2
109.66.154.212	Israel	147.237.72.156	aman.idf.il	Unauthorized URL Access to www.aman.idf.il/console/core/doc_mgr/undefined	Block	2
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Untraceable SSL Sessions: Protocol violation (SSL_CONN_APPLICATION_DATA_EXCHANGE)	None	2
178.32.53.53	United Kingdom	147.237.77.216	dover.idf.il	Distributed Unauthorized URL Access on www.idf.il/templates/article/watch	Block	2
37.26.149.128	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	2
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Multiple Unauthorized URL Access from 94.242.228.108	Block	2
66.249.78.216	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	2
68.180.230.224	United States	147.237.76.31	nakchal.idf.il	Parameter Type Violation PageNum in www.nakhal.idf.il/1111-he/nakhal.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Malformed HTTP Header Line	Block	1
85.10.210.199	Germany	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/watch	Block	1
37.46.35.113	Israel	147.237.72.156	aman.idf.il	SSL Untraceable Connection - Open Mode	None	1
157.55.39.48	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to www.cogat.idf.il/size220x0/sip_storage	Block	1
94.242.228.108	Luxembourg	147.237.77.216	dover.idf.il	Unauthorized URL Access to www.idf.il/templates/article/u1t4pvovmkk	Block	1
79.181.100.172	Israel	147.237.76.42	refuah.idf.il	Distributed Unauthorized URL Access on 147.237.76.42/1518-he/refuah.aspx	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Illegal HTTP Version Ãˆ[[#30]][[#14]]P_Â«[[#14]]Â®W[[#16]]Â‡ rBÃªÃ·=[[#11]]Ã‹VI+Â¿Â Â¬ÃžÃ˜Ã“Ã–RÃˆQÂ©Ã®Ã‹XÃ¨Â¾ÃŽÂ¨Â„Â'Â¹ÃŸ Ã½LÃ®gÂ¼[[#26]]`Qa[[#31]]Ã?ÃŒgÃšÂžÂ¯@Ã™Ã'Â¯b_Â™Âž"[[#18]]ÂŽ 2Â§ÃšÃ˜Â¡Ã"`6nÃ?NÃ´ÂˆÂ¾\Ã-A@^[[#24]]Ã…Â¡Â-SÃ"[baÃ¾ÂœÃ?Ã‡ Â£[[#22]][[#5]]Â'Ã?Â†Âž&Ãµ{Â¿{Ã· h.Â«o7rKÃ-/^Ã–Ã-Ã?(:*Â³[[#27]]Â¥p2Ã-Ã¹gVZÂ„8{J[[#20]]~O Â-k[[#6]]Â‰jÂ"{#Ã¶>Â€[[#11]][[#15]] lQÃž4Â±T[[#16]]LÂ"Â¼Â" wÂ©Â£Â¡Ã²Ã™\vflÂ¸Â-Â©!Ã¬:Â›s@_?Ã‡Â„w0Ã" [[#0]][[#1]]{D[[#11]][[#18]]Â–Ã?@Â¡Â™Â¯XÃ³Ã€Ã´+Ã¥Ã Ã…NÃŒ i"Â-[[#28]]Ã…[[#31]]&Zhw2[[#22]]•[[	Block	1
66.249.78.236	Israel	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/sip_storage/files/8/3338.jpg	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Header Name	Block	1
89.139.161.34	Israel	147.237.72.166	aka.idf.il	Unknown Parameter ctl00$ctl00$cphMain$TochenPlaceHolder$ctl13$ctl01$ctl03$cblQuestion$41 in aka.idf.il/main/giyus/questionnaire.aspx	None	1
46.19.85.44	Israel	147.237.77.216	dover.idf.il	Malformed URL	Block	1
84.111.38.42	Israel	147.237.72.166	aka.idf.il	Distributed Illegal Byte Code Character in Method	Block	1
217.194.198.104	Israel	147.237.72.166	aka.idf.il	Distributed Malformed URL	Block	1
85.250.234.87	Israel	147.237.77.234	halag.idf.il	Unauthorized URL Access to 147.237.77.234/images/shared/bullet1.gif	Block	1
46.19.86.158	Israel	147.237.0.19	madim.atal.idf.i	Distributed Suspicious Response Code	Block	1
207.46.13.192	United States	147.237.77.176	matpash.idf.il	Unauthorized URL Access to 147.237.77.176/	Block	1
37.105.201.147	Saudi Arabia	147.237.77.216	dover.idf.il	Admin Blocking	Block	1
157.55.39.160	United States	147.237.76.42	refuah.idf.il	Unauthorized URL Access to 147.237.76.42/robots.txt	Block	1
80.246.137.99	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
2.54.3.92	Israel	147.237.77.243	mobile.idf.il	Distributed Suspicious Response Code	Block	1
95.86.109.228	Israel	147.237.76.86	navy.idf.il	Unauthorized URL Access to www.navy.idf.il/1132-8204-he/navy.aspx&sa=u&ved=0ahukewik_pqk-exkahwcxbokhekvchaqfggnmae&sig2=whtwyqmang_i9iab08oftw&usg=afqjcng82vvdpmo8xoz-1oxgwnrfhm56pg	Block	1

02-07-2016-17:04:07 to 02-07-2016-18:04:07